

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN RE APPLICATION OF THE)
UNITED STATES OF AMERICA FOR) Case No. 22-mc-
AN ORDER PURSUANT TO)
18 U.S.C. § 2703(d)) **Filed Under Seal**

)

**APPLICATION OF THE UNITED STATES
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)**

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an Order pursuant to 18 U.S.C. § 2703(d). The proposed Order would require Microsoft, an email service provider headquartered in Redmond, Washington, to disclose certain records and other information pertaining to the email account as described in Part I of Attachment A. The records and other information to be disclosed are described in Part II of Attachment A to the proposed Order. In support of this application, the United States asserts:

LEGAL BACKGROUND

1. Microsoft is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Accordingly, the United States may use a court order issued under § 2703(d) to require Microsoft to disclose the items described in Part II of Attachment A. *See* 18 U.S.C. § 2703(c)(2) (Part II.A of Attachment A); 18 U.S.C. § 2703(c)(1) (Part II.B of Attachment A).

2. This Court has jurisdiction to issue the proposed Order because it is “a court of competent jurisdiction,” as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(d). Specifically,

the Court is a district court of the United States that has jurisdiction over the offense being investigated. *See* 18 U.S.C. § 2711(3)(A)(i).

3. A court order under § 2703(d) “shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). Accordingly, the next section of this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation.

THE RELEVANT FACTS

4. The United States is investigating Nadia Alawa and her charity, NuDay Syria, for potential donor fraud, tax fraud, export violations, and related offenses. The investigation concerns possible violations of, *inter alia*, 50 U.S.C. §§ 1701-1708 (International Emergency Economic Powers Act (“IEEPA”)); 31 U.S.C. § 5322 (Willfully Failing to file a Foreign Bank and Financial Accounts Report, or FBAR); 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 554 (Smuggling From the United States); 26 U.S.C. § 7206(1) (Fraud and False Statements); 13 U.S.C. § 305 (Unlawful Export Information Activities); and 18 U.S.C. § 371 (associated conspiracy offenses) (collectively, the “Subject Offenses”)

5. The following paragraphs briefly summarize the grounds for the Government’s belief that the records sought are relevant and material to the ongoing investigation. For complete reference, however, the Court may also review the affidavit of FBI Special Agent Corey Howe, which was the basis for multiple related search warrants in this investigation. *See*

21-mj-285-AJ (authorizing search of Alawa's residence); 21-mj-286-AJ (authorizing search of NuDay's warehouse); 21-mj-287-AJ (authorizing search of Alawa herself).

6. Over the last few years, law enforcement has been investigating Alawa and NuDay for charity fraud. Alawa is the founder and operator of NuDay, a non-profit charity.

7. However, to maintain its tax-exempt status, NuDay has made likely fraudulent representations to donors, the New Hampshire Attorney General's Charitable Trust Unit (CTU), and the Internal Revenue Service (IRS).

8. At a very high level, NuDay solicits donations of cash to operate programs in Syria to assist the refugee population there. However, donated funds appear to have been misused. For example, NuDay gives donors the option to sponsor orphans and pay for schools operated by the charity. With respect to the former, NuDay would infrequently give updates about sponsored orphans and, on at least one occasion, claimed the sponsored orphan was "lost" after the donor asked for an update. With respect to the latter, NuDay subsequently admitted to investigators that it had not operated schools for several years.

9. Between May 2017 and January 2021, approximately \$4.8 million of funds NuDay solicited were wired overseas to a bank account at Ziraat Bank in Turkey. The account is held in the name of an entity called Yeni Suriye Istikbal Dernegi (Yeni). Previously, NuDay claimed that Yeni was NuDay's Turkish entity and that the Ziraat Bank account was NuDay's overseas operating account. However, on April 27, 2022, NuDay represented to the Commerce Department, Justice Department, Treasury Department, and Census Bureau that NuDay had no ownership interest in, control of, or access to Yeni funds. Therefore, at minimum, NuDay was wiring large amounts of cash to an overseas account of which it did not control.

10. Prior to the wires to Ziraat Bank, Alawa made large bulk cash withdrawals in the United States from an account held in NuDay's name.

11. NuDay also solicits donations of goods and supplies for shipment to Syria in large containers. NuDay asks volunteers to help package the containers. However, a confidential witness reported that most items packaged in these containers are used goods with little to no resale value and that it would be cheaper for NuDay to simply buy new goods in Turkey for transport into Syria.

12. Despite this, NuDay claimed year after year on tax returns that it received tens of millions of dollars in in-kind donations. For example, in 2018, NuDay claimed to have received \$40 million in in-kind donations. Of that amount, \$12 million alone purportedly came from the International Medical Equipment Collaborative. Ellen Oliver, the former CEO of IMEC, said that was false and that true amount of IMEC's in-kind donations was far closer to \$12,000 than \$12 million. And in 2019, NuDay claimed to have received \$70 million in in-kind donations. NuDay's own estimates placed the average value of each container shipped overseas at millions of dollars, which is contradicted by the reports of the confidential witness in the prior paragraph.

13. All shipments destined for Syria, regardless of value, required a shipping license. NuDay did not obtain the requisite licenses for its shipments between 2013 and 2019.

14. An export valued over \$2,500 or for which an export license is required (again, including all shipments destined for Syria) require an Electronic Export Information (EEI), formerly known as a Shipper's Export Declaration. An EEI discloses information such as the ultimate end-user or destination of the export. It is important for exporters to file truthful EEIs so that the Commerce Department can enforce U.S. export laws and regulations. NuDay did not even submit an EEI until 2021 after law enforcement began investigating NuDay's activities.

15. NuDay therefore likely violated applicable export laws and regulations.

16. NuDay usually pays a freight forwarder called AJ Worldwide Services to ship the containers to Mersin, Turkey. Another company called Safir Forwarding then transports the containers from Turkey to Syria. NuDay has made payments directly to both AJ Worldwide Services and Safir Forwarding. However, NuDay has also made direct payments to a Safir employee named Nihal Kahil for unknown reasons.

17. On May 12, 2022, Special Agent Christine Chambers of the Department of Commerce's Office of Export Enforcement contacted another freight forwarder called Omega Global Logistics. Omega Global Logistics confirmed that in September 2021 it shipped a NuDay container with an ultimate consignee and destination agent of "Passador" located at the Airport Road Zarzour Center, 2nd Floor in Beirut, Lebanon.

18. The only contact information for Passador that Omega had was an email address: passador2020@hotmail.com. No EEI was filed for this shipment.

19. Open source searches of Passador and that address did not yield any positive results.

20. In summary, the above facts show that Alawa and NuDay have been engaging in criminal conduct, including export violations, and that they have shipped a container containing unknown goods to Lebanon to an unknown entity. The information sought in this order would help law enforcement determine whether the intended recipient of this container is a legitimate entity and whether further export violations were committed.

REQUEST FOR ORDER

21. The facts set forth in the previous section show that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are

relevant and material to an ongoing criminal investigation. Specifically, these items will help the United States to identify and locate the individual(s) who are responsible for the events described above, and to determine the nature and scope of their activities. Accordingly, the United States requests that Microsoft be directed to produce all items described in Part II of Attachment A to the proposed Order.

22. The United States further requests that the Order require Microsoft not to notify any person, including the subscribers or customers of the account(s) listed in Part I of Attachment A, of the existence of the Order for a time period of one year. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue “an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.” *Id.* In this case, such an order would be appropriate because the attached court order relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the attached court order will seriously jeopardize the investigation or unduly delay a trial, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, or change patterns of behavior.

23. The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of

the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

JANE E. YOUNG
UNITED STATES ATTORNEY

By: /s/ Alexander S. Chen
Alexander S. Chen, SAUSA
53 Pleasant Street, 4th Floor
Concord, NH 03301
(603) 225-1552
alexander.chen@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN RE APPLICATION OF THE)
UNITED STATES OF AMERICA FOR) Case No. 22-mc
AN ORDER PURSUANT TO)
18 U.S.C. § 2703(d))

) **Filed Under Seal**

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2703(d), requesting that the Court issue an Order requiring Microsoft, an electronic communications service provider and/or a remote computing service headquartered in Redmond, Washington, to disclose the records and other information described in Attachment A to this Order.

The Court finds that the United States has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

The Court determines that there is reason to believe that notification of the existence of this Order will seriously jeopardize the ongoing investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. *See* 18 U.S.C. § 2705(b)(2), (3), (5).

IT IS THEREFORE ORDERED, pursuant to 18 U.S.C. § 2703(d), that Microsoft shall, within ten days of the date of this Order, disclose to the United States the records and other information described in Attachment A to this Order.

IT IS FURTHER ORDERED under 18 U.S.C. § 2705(b) that Microsoft shall not disclose the existence of the application of the United States, or the existence of this Order of the Court, to the subscribers of the account(s) listed in Attachment A, or to any other person, for one year,

except that Microsoft may disclose this Order to an attorney for Microsoft for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court.

Hon. Andrea Johnstone
United States Magistrate Judge

Date

ATTACHMENT A

I. The Account(s)

The Order applies to certain records and information associated with the following email account:

passador2020@hotmail.com

II. Records and Other Information to Be Disclosed

Microsoft is required to disclose the following records and other information, if available, to the United States for each account or identifier listed in Part I of this Attachment (“Account”), for the time period January 1, 2020 to the present, regardless of whether such information is located within or outside of the United States:

A. The following information about the customers or subscribers of the Account:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
3. Local and long distance telephone connection records (including records of text messages sent and received);
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses);
7. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

B. All records and other information (not including the contents of communications) relating to the Account, including:

1. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses; and
2. Information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers).

The Provider is hereby ordered to disclose the above information to the government within 10 days of issuance of this Order.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by [PROVIDER], and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of [PROVIDER]. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS, SUCH AS: pages / CD(s) / megabytes]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of [PROVIDER], and they were made by [PROVIDER] as a regular practice; and

b. such records were generated by [PROVIDER]'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of [PROVIDER] in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by [PROVIDER], and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature